PTO/SB/17 (12-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2005

Effective 10/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500.00

Complete if Known	
Application Number	09/675,399
Filing Date	September 29, 2000
First Named Inventor	Carl BILICSKA
Examiner Name	Hassan Mahmoudi
Art Unit	2165
Attorney Docket No.	129250-001034/US

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 50-3777

Deposit Account Name: CAPITOL PATENT & TRADEMARK LAW FIRM, PLLC

The Director is authorized to: *(check all that apply)*
☐ Charge fee(s) indicated below ☒ Credit any overpayments
☒ Charge any additional fee(s) during the pendency of this application
☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1011	300	2011	150	Utility filing fee	
1012	200	2012	100	Design filing fee	
1013	200	2013	100	Plant filing fee	
1014	300	2014	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims		-20 **	= 9 prev. paid for	X		=	0
Independent Claims		-3 **	= 4 prev. paid for	X		=	0
Multiple Dependent						=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500
1403	1000	2403	500	Request for oral hearing	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1500	2453	750	Petition to revive – unintentional	
1501	1400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17 (q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
Other fee (specify) ____					

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($)500

4. SEARCH/EXAMINATION FEES

1111	500	2111	250	Utility Search Fee
1112	100	2112	50	Design Search Fee
1113	300	2113	150	Plant Search Fee
1114	500	2114	250	Reissue Search Fee
1311	200	2311	100	Utility Examination Fee
1312	130	2312	65	Design Examination Fee
1313	160	2313	80	Plant Examination Fee
1314	600	2314	300	Reissue Examination Fee

SUBTOTAL (4) ($)0

SUBMITTED BY

Complete (if applicable)

Name (Print/Type)	John E. Curtin	*Registration No. (Attorney/Agent)*	37,602	*Telephone*	(703) 266-3330
Signature				*Date*	May 1st, 2006

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

IN THE U.S. PATENT AND TRADEMARK OFFICE

Appellants:	Carl BILICSKA et al.
Application No.:	09/675,399
Art Unit:	2165
Filed:	September 29, 2000
Examiner:	Hassan Mahmoudi
For:	AUTOMATED AUTHENTICATION HANDLING SYSTEM
Attorney Docket No.:	129250-001034/US

APPLICANT'S BRIEF ON APPEAL

MAIL STOP APPEAL BRIEF - PATENTS
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

May 1, 2006

TABLE OF CONTENTS

APPELLANT'S BRIEF ON APPEAL

I. REAL PARTY IN INTEREST:

The real party in interest in this appeal is Lucent Technologies Inc. Assignment of the application was submitted to the U.S. Patent and Trademark Office on September 29, 2000, and recorded on the same date at Reel 011176, Frame 0834.

II. RELATED APPEALS AND INTERFERENCES:

There are no known appeals or interferences that will affect, be directly affected by, or have a bearing on the Board's decision in this Appeal.

III. EVIDENCE SUBMITTED UNDER CFR 1.130, 1.131, OR 1.132:

None.

IV. DECISIONS RENDERED BY THE COURT OR THE BOARD IN RELATED APPEALS AND INTERFERENCES:

None.

V. STATUS OF CLAIMS:

Claims 1-14 are pending in the application, with claims 1 and 9 being written in independent form.

Claims 1-2, 4, 6-11 and 13-14 remain finally rejected under 35 U.S.C. §103(a). The Examiner has indicated that the subject matter of claims 3, 5 and 12 is allowable if these claims are re-written in independent form. Appellants reserve their right to further prosecute these claims upon issuance of a decision by the Board. Claims 1-2, 4, 6-11 and 13-14 are being appealed.

VI. STATUS OF AMENDMENTS:

A Request for Reconsideration ("Request") was filed on February 3, 2006. In an Advisory Action dated February 27, 2006, the Examiner stated that the Request was considered and Appellant's amendments entered; however, the Request did not place the application in condition for allowance.

VII. SUMMARY OF CLAIMED SUBJECT MATTER:

(i) Overview of the Subject Matter of the Independent Claims.

The present inventions are directed at methods that allow users to initiate a single authentication process with one authentication server which, in turn, automatically initiates authentication processes with other application servers in a network that a user is permitted to access. For example, the authentication server may establish a two-way, trusted communication link between the user and application servers that are selected from a list using a client/user identifier. (paraphrasing page 2 of specification; see also, for example, p. 4, line 25 to p. 5, line 1; p. 6, lines 10-18 and 21-25; p.7, lines 16-18).

(ii) Additional Text from the Specification in Support of the Claims.

In more detail, with reference to Figure 4 (Appendix B) an automated authentication handling system 100 according to the present invention includes a plurality of clients 102-104 that are connected via a network 106 such as the Internet or an intranet. Similarly, a plurality of application servers 108-110 are connected to the network. Advantageously, the present invention includes an authentication server 111 connected to the network 106 and

configured to authenticate clients and application servers to establish a communication link 112-114 directly between the clients 102-104 and the application servers 108-110. For purposes of illustrating the features of this invention, the invention will be described in the context of Internet protocols and more particularly the HyperText Transfer Protocols (HTTP). However those skilled in the art will appreciate that the features of this invention may be utilized on any network protocol platform. (See specification, p. 4)

The authentication server 111 generally may include conventionally available hardware and software for connecting to a network and interacting with communication protocols used by the network. For example, when used over the Internet the server may include web server software of the type published by Apache Digital Corporation of Durango, CO. The Apache web server software can be easily configured to include specialized tasks using software compatible with the Common Gateway Interface (CGI). The authentication server of the present invention includes two specialized tasks or modules (Figure 5; Appendix C), namely, an identifier engine 116 and a communication initiation engine 118. (See specification, p. 4)

With continued reference to Figure 5, the identifier engine 116 includes a database 120 having a plurality of client identifier records 122 and a plurality of application server records 124. Each of the client identifier records is related to one or more of the application servers. The relationships of the client identifier records to the application servers is preferably tailored to the desired relationships between the clients 102-104 and the applications servers 108-110. As a result, for each client identifier in the database a listing of application servers authorized by the client identifier may be generated in a report. When a client provides a client identifier, a report 126 containing a listing of the application servers authenticated for access by the client identifier is generated and sent to the client. The report is preferably generated in a hyper-text format such as the hyper-text markup language (HTML) used by

HTTP. The hyper-text format is embedded with a link for each application server in the listing. The link addresses the communication initiator engine on the authentication server and includes a request to establish a communication link with an associated application server. This request is preferably in the form of an HTML POST command in which the application server is provided in the hypertext document in an encrypted format. This prevents a user (client) from modifying the hypertext document to change access privileges. (See specification, pp. 4-5)

Accordingly, the hypertext report provides a user interface 128 that may be used by a client when the hypertext document is loaded by a conventional web browser of the type such as Explorer published by Microsoft or Navigator published by Netscape. The user interface 128, when used by a client having a conventional graphical user interface such as Microsoft Windows or Apple Macintosh OS, may appear as a separate window that can be accessed when needed by a user. Using the HTML language it will be appreciated that a number of user interface configurations may be used including, but not limited to, pull-down menus or hypertext listings. Once the document has been sent to the client, no further authentication by the user is required to access the application servers contained in the listing. This user interface provides a great advance over existing authentication methodologies as the user does not have to provide a separate authentication for each of the application servers. Furthermore, it will be appreciated that authentication administration can be handled by a single server rather than having separate authentication administrators for each of the application servers. A client's communications with the authentication server may include a Secure Socket Layer (SSL) session link, cookies or other conventional security measures that may be used to verify continued communication from the client to the authentication server.

In another embodiment, the client identifier is further related to session assignment information for each of the application servers. The session

assignment can include information for limiting client access to the features on each of the application servers as well as session timeout information. It will be appreciated that the session assignment information may be specifically tailored to access the capabilities of each of the application servers. When the report in hypertext format is sent to the client the link designating a request for an application server may be encoded with application server information in an encrypted format. (See specification, pp. 5-6)

The communication initiator engine 118 is responsive to a request from the client to establish a communication link 130 with one of the application servers. The communication initiator engine 118 preferably receives the encrypted request information, illustrated by line 132, and decrypts the information. The requested information is preferably compared to a look-up table in which each application server and session assignment information is stored as a separate listing. The authentication server matches the client's request with the appropriate listing. The listing is combined with the client's address. The client address and session information are then encrypted by the communication initiator engine and transmitted to the application server, illustrated by line 134, again using an HTTP POST method. (See specification, p. 6)

The application server receives the information transmitted in the post command and includes a verification engine 136, preferably running as a CGI script on the application server. It should be noted that the verification engine 136 does not verify that the information was received by checking the IP address of a trusted authentication server, rather it decrypts the posted information and uses a shared secret data field to verify the authentication server. It will be appreciated by those skilled in the art that such verification allows for dynamic, IP addressing of the authentication server. The encryption/decryption method used by the present invention may vary; however, a public key/private key methodology is preferred. Thus, the

decryption of information from the authentication server is decrypted using a private key contained on the application server. The decrypted information includes the session assignment information and the client's address. The information also preferably includes a verification record that contains secret information shared exclusively between the authentication server and the application as a further verification that the information was transmitted from a trusted source. If the verification fails, an error message is returned and no further action is taken. (See specification, pp. 6-7)

If the verification is cleared, a Uniform Resource Locator (URL) is generated containing a unique address for the client to access the application and further includes session assignment information that is encrypted by the verification engine prior to transmittal. The URL is then transmitted to the Authentication Server, illustrated by line 140, which in turn forwards the URL directly to the client, illustrated by line 142. Once received by the client, the URL is addressed back to the application server directly from the client along with the encrypted session information initiating the communication link 134. The application server again decrypts the session information and verifies that the URL request was transmitted from the IP address of the client 102 originally transmitted to the application server by the authentication server. The application server also verifies that a session timeout time is still valid. The application server then establishes a trusted communication link 134 directly with the client. The trusted communication link 134 may include security such as an SSL communications link; or a cookie containing the relevant session information may be placed on the client's computer. The cookie is used by the application to verify the user and provide other information relevant to the session such as session time-out information. The URL then redirects the client to the main session application page of the web site. (See specification, p. 7)

With reference to Figure 6 (Appendix D), signaling between a client 102 and an application server 108 using an authentication server 108 includes initiating a login request from the client to the authentication server, illustrated by line 125. The authentication server replies with a report in hypertext listing the application servers authorized to be accessed by the client, illustrated by line 126. A client selects an application server for access and submits a request to the authentication server, illustrated by line 132. The authentication server forwards the request to the application server, illustrated by line 134. The application server responds and confirms access as illustrated by line 140. The authentication server forwards the selection authorization to the client 102, illustrated by line 142. The client 102 and application server 108 then establish and communicate via a trusted communication link, illustrated by line 130. (See specification, pp. 7-8)

VIII. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:

Appellants seek the Board's review and reversal of the rejections of claims 1,2,4, 6-11 and 13-14 under 35 U.S.C. §103(a).

IX. ARGUMENTS:

A.) The Section 103 Rejections

Claims 1, 2, 4, 6-11 and 13-14 were rejected under 35 U.S.C. §103(a) as being unpatentable over Reed et al., U.S. Patent No. 5,862,325 ("Reed") in view of Ramasubramani et al., U.S. Patent No. 6,233,577 ("Ramasubramani"). Appellants disagree and respectfully request that the Board reverse the decisions of the Examiner and allow claims 1, 2, 4, 6-11 and 13-14 for at least the following reasons.

Initially, Appellants note that it is not clear how the Examiner is now applying Reed and Ramasubramani to reject the claims. In the Final Office Action the Examiner stated:

> "Reed et al does not teach a two-way trusted communications link or access by an authenticated user to a list of application servers associated with a client identifier."(page 3, 1st full paragraph).

In the latest Advisory Action, however, the Examiner appears to have changed his mind. In sum, the Examiner's position is confusing to the Appellants. Appellants submit that the proper course is for the Examiner to withdraw the finality of the rejections and re-open prosecution to make his position clear and to allow the Applicants to respond accordingly.

That said, the Appellants will attempt to respond now bearing in mind the statements made by the Examiner in the Advisory Action.

The present position of the Examiner (as set forth in the Advisory Action) appears to be that Reed discloses "an authentication server" that is "adapted to establish a two-way communication link". In addition, the Examiner now appears to be taking the position that Reed also discloses an authentication server that, through such a two-way link, permits an authenticated user access to a list of application servers thought his is not entirely clear to the Appellants. Therefore, Appellants presume that the Examiner is acknowledging that Reed does not disclose an authentication server that, through an authenticated two-way link, permits an authenticated user access to a list of application servers associated with a client identifier, as in the claims of the present invention. To make up for this deficiency the Examiner appears to be relying upon Ramasubramani. That said, it is not at all clear to the Appellants that the Examiner is relying on Ramasubramani at all.

Nonetheless, Appellants note that Ramasubramani does not disclose a list of application servers that are associated with a client identifier. The excerpt from the Abstract referenced by the Examiner in the Final Office Action (p. 3) refers to a plurality of secure servers that, it appears, may be accessed

using a plurality of certificates. Ramasubramani does not disclose or suggest that multiple servers are associated with the same certificate or client identifier.

Appellants also note that the combination of Reed and Ramasubramani apparently relied upon by the Examiner is impermissible because it would appear to require Ramasubramani to change its principle of operation.

As set forth in the claims, the same authentication server establishes a two-way trusted communication link and allows an authenticated user to access a list of application servers associated with a client/user identifier . In contrast, Ramasubramani discloses two servers neither one of which is responsible for both establishing a trusted link and allowing a user access to a list of application servers. The first server in Ramasubramani is a proxy server (see Abstract); the second is a merchant's authentication server (see FIG. 1 and the excerpts in column 4). It is the proxy server that reserves certificates for a client, which the client may later send to the merchant's authentication server. The proxy server in Ramasubramani does not establish a two-way trusted communication link; it only reserves certificates. The establishment of the link is left up to the merchant's authentication server. While such a server may establish a link, it does not allow the user access to a list of application servers. Further, the fact that a merchant's authentication server may allow a client access to its server is not akin to, or suggestive of, allowing a client access to a list of application servers, as in the claims of the present invention. In order to properly combine Reed and Ramasubramani, the principle of one or both of the servers in Ramasubramani would have to be changed to both establish a trusted link and allow a user access to a list of application servers. This, as the Examiner knows well, is impermissible.

Accordingly, Applicants respectfully submit that the claims of the present invention would not have been obvious to one of ordinary skill in the art upon reading the disclosures of Reed and Ramasubramani because taken separately,

or in combination, neither discloses or suggests an authentication server that both establishes a two-way trusted communication link and allows an authenticated user access to a list of application servers, as in the claims of the present invention.

X. CONCLUSION:

Appellants respectfully request that the members of the Board reverse the decisions of the Examiner, withdraw the pending rejections and allow claims 1, 2, 4, 6-11 and 13-14.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 50-3777 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

XI. EVIDENCE APPENDIX

None.

XII. RELATED PROCEEDINGS APPENDIX

None.

Respectfully submitted,

CAPITOL PATENT & TRADEMARK LAW FIRM, PLLC

By: _____

John E. Curtin, Reg. No. 37,602
(703)266-3330
P.O. Box 1995
Vienna, VA 22183

JEC:

APPENDIX A

CLAIMS APPENDIX

1. An automated authentication handling system for use by clients on a network comprising:

an authentication server adapted to establish a two-way trusted communication link for access by an authenticated user to a list of application servers associated with a client identifier.

2. The automated authentication handling system of claim 1 wherein said authentication server includes:

an identification engine configured to maintain collections of session assignments for accessing said application servers, each of said session assignment collections being associated with the client identifier.

3. The automated authentication handling system of claim 2 wherein said identification engine is adapted to receive client identifiers from said clients to establish authenticated users and responsive thereto to provide a user interface to access said application servers according to said associated session assignments.

4. The automated authentication handling system of claim 1 wherein said authentication server includes:

a communication initiator engine configured to establish the trusted communication link between said authenticated users and an application server on said list.

5. The automated authentication handling system of claim 3 wherein said authentication server includes:

a communication initiator engine configured to establish the trusted communication link defined to one of said session assignments between said authenticated users and said application server.

6. The automated authentication handling system of claim 1 wherein said session assignments include data fields selected from the group consisting of session timeout and application access level.

7. The automated authentication handling system of claim 1 wherein said client identifier includes a user id and password.

8. The automated authentication handling system of claim 1 wherein said authentication server includes a processor under the control of software to:

receive an authentication signal from said client;

provide an application access interface to said client in response to said authentication signal; and

establish the trusted communication link between said client and an application server selected from said application access interface.

9. A method for automatically authenticating a client for a plurality of application servers comprising the steps of:

providing an authentication server;

identifying clients for access to said application servers by said authentication server; and

establishing a two-way trusted communication link between a client and an application server selected from a list of application servers associated with a client identifier.

10. The method of claim 9 wherein said identifying step includes:

providing session parameters for each of said identified clients for at least one of said application servers.

11. The method of claim 9 wherein said identifying step includes:

providing a user interface to said identified clients for accessing said application servers.

12. The method of claim 10 wherein said establishing step includes:

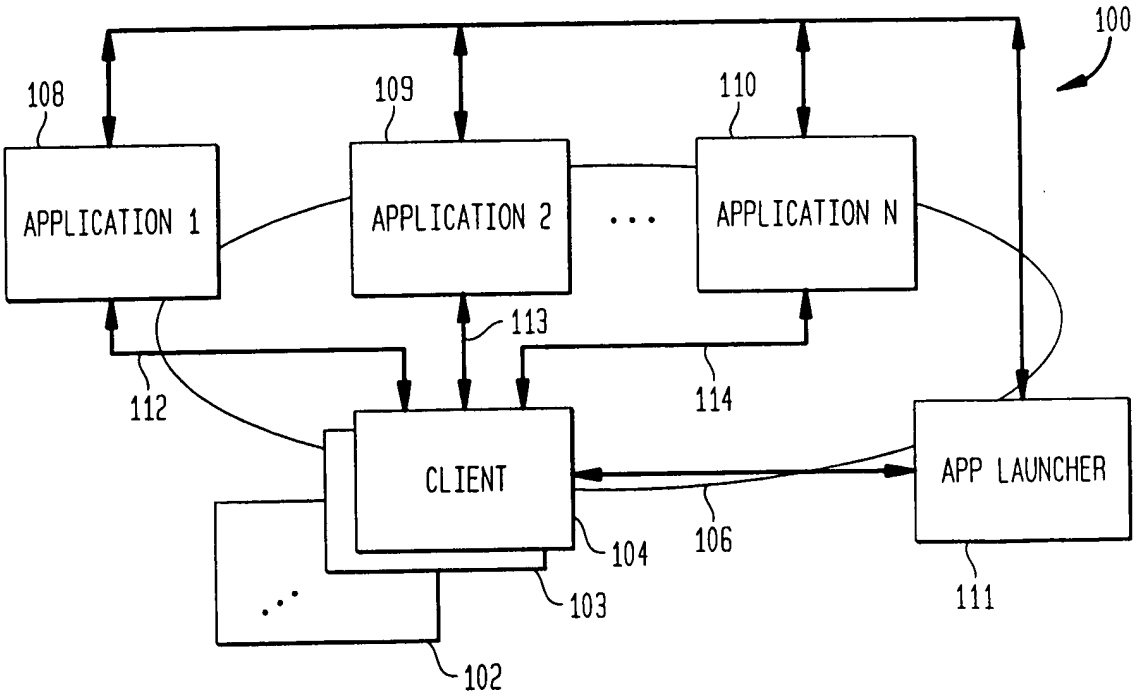
using said session parameters to establish said trusted communication link.

13. The method of claim 11 wherein said user interface includes a listing of application servers and said establishing step is initiated following a selection of an application server by a user from said user interface.

14. The method as in claim 1 further comprising a plurality of application servers connected to said network, each requiring authentication for access.

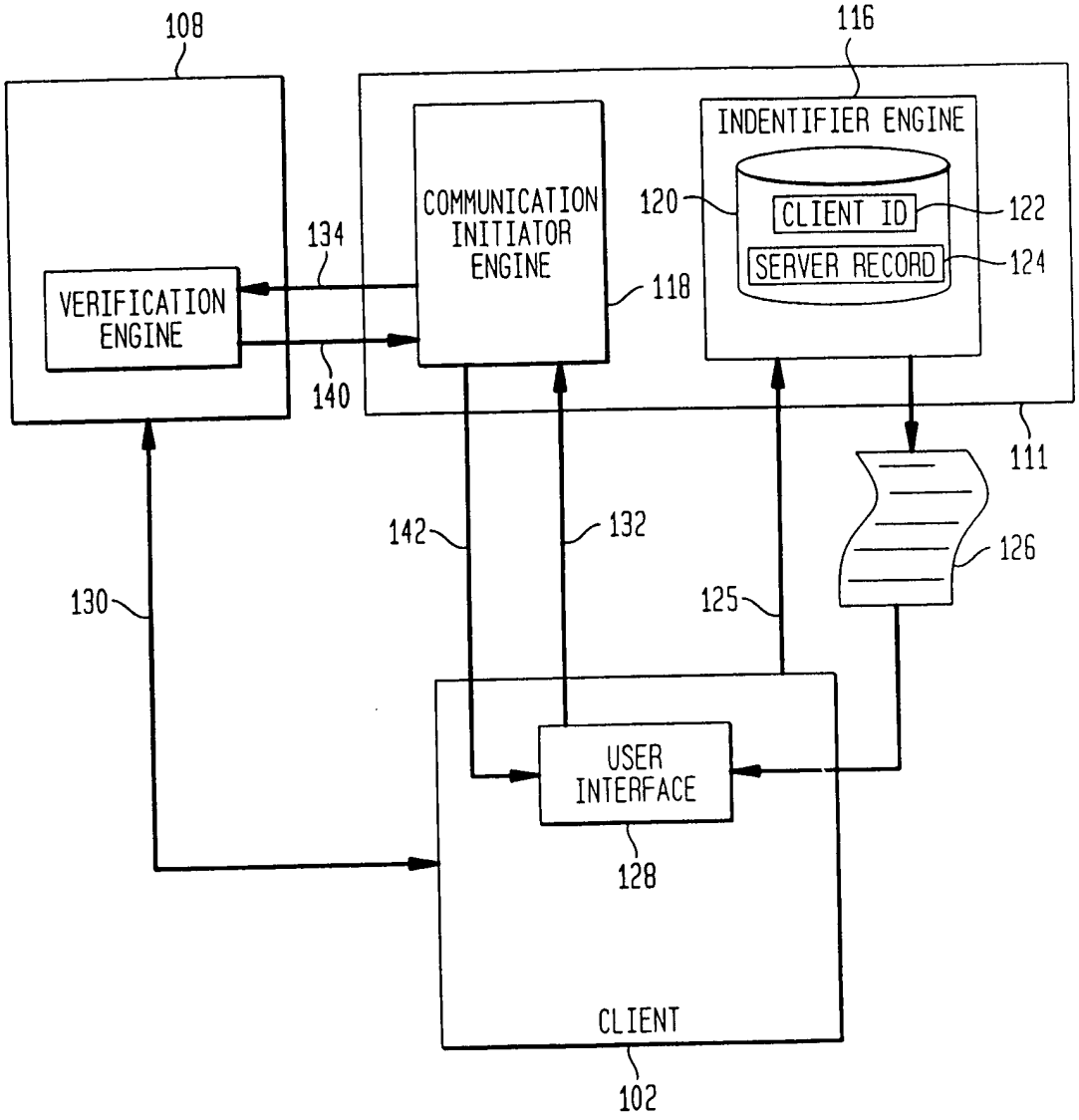
Appdx. B

FIG. 4



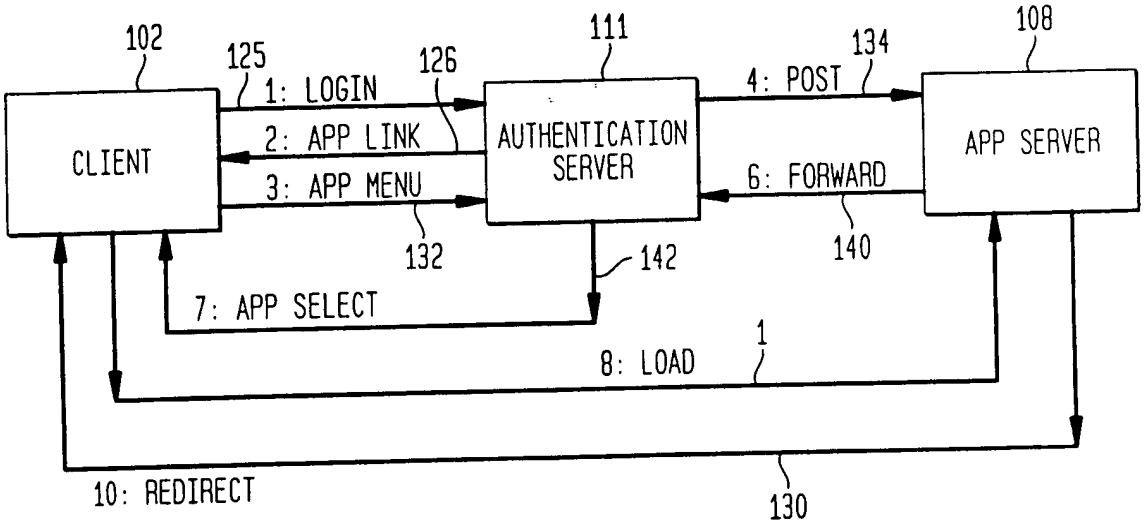
Appdx. C

FIG. 5


108
116
INDENTIFIER ENGINE
COMMUNICATION INITIATOR ENGINE
120
CLIENT ID
122
SERVER RECORD
124
134
VERIFICATION ENGINE
118
140
111
142
132
126
130
125
USER INTERFACE
128
CLIENT
102

Appdx. D

FIG. 6


102
125
1: LOGIN
126
111
134
4: POST
108
CLIENT
2: APP LINK
AUTHENTICATION SERVER
APP SERVER
3: APP MENU
6: FORWARD
132
142
140
7: APP SELECT
1
8: LOAD
10: REDIRECT
130